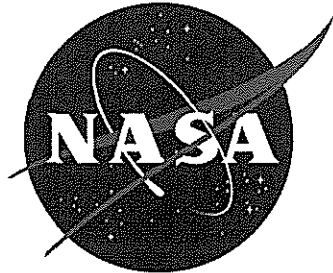


# NASA Information Technology Requirement



**NITR 2810-21**

Effective Date: April 28, 2009

Expiration Date: May 16, 2011

---

## **System and Services Acquisition Policy and Procedures**

---

Responsible Office: Office of the Chief Information Officer

## **Table of Contents**

## **Change History**

## **PREFACE**

- P.1 PURPOSE
- P.2 APPLICABILITY
- P.3 AUTHORITY
- P.4 APPLICABLE DOCUMENTS
- P.5 MEASUREMENT AND VERIFICATION
- P.6 CANCELLATION

## **1.0 REQUIREMENT**

- 1.1 System and Services Acquisition Policy
- 1.2 Procedures

## **APPENDIX A. Descriptions**

## **APPENDIX B. Acronyms**

## **APPENDIX C. NASA Information Technology (IT) Waiver Process**

## **Distribution**

**NODIS**

## Change History

NITR-2810-21, System and Services Acquisition Policy and Procedures

Change Number	Date	Change Description

## **PREFACE**

### **P.1 PURPOSE**

To provide the NASA information system and services acquisition policy and procedures needed to meet the current National Institute of Standards and Technology (NIST) requirements.

### **P.2 APPLICABILITY**

This NITR applies to unclassified information systems at NASA Headquarters and Centers, including Component Facilities and Technical and Service Support Centers. To the extent specified in their respective contracts or agreements, it applies to the NASA Jet Propulsion Laboratory, other contractors, grant recipients, or parties to agreements for information systems that they use or operate on behalf of the Agency or that support the operations and assets of the Agency.

### **P.3 AUTHORITY**

Reference Paragraph P.3, NPR 2810.1A, Security of Information Technology.

### **P.4 APPLICABLE DOCUMENTS**

- a. NPR 2810.1, Security of Information Technology.
- b. NPR 1382.1, NASA Privacy Procedural Requirements.
- c. NPR 1600.1, NASA Security Program Procedural Requirements.
- d. NPD 2540.1, Personal Use of Government Equipment Including Information Technology.
- e. NPR 7120.5, NASA Space Flight Program and Project Management Requirements.
- f. NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements
- g. NASA FAR Supplement 1852.204-76, NASA IT Security Clause.
- h. Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.
- i. NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.
- j. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.
- k. NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems.
- l. NIST SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.
- m. NIST SP 800-64, Security Consideration in the System Development Lifecycle.

n. NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process.

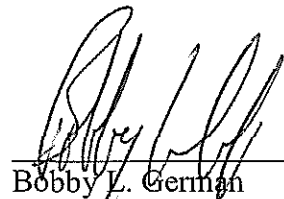
## **P.5 MEASUREMENT AND VERIFICATION**

a. Annual certification of the Agency common security control, SA-1, System and Services Acquisition Policies and Procedures of the NIST System and Services Acquisition (SA) family of security controls.

b. Annual assessment of the Agency common security control SA-1 by the Information System Owner (ISO) as part of the system Continuous Monitoring requirement.

## **P.6 CANCELLATION**

a. The next version of NPR 2810.1 cancels this NITR.



Bobby L. German  
Chief Information Officer (Acting)

7/28/09  
Date

## **1.0 REQUIREMENT**

### **1.1 System and Services Acquisition Policy**

1.1.1 NPR 2810.1A, Chapter 10 provides the NASA baseline System and Services Acquisition Policy.

1.1.2 The NASA System and Services Acquisition Policy and Procedures shall be consistent with NASA policies and procedures, applicable laws, executive orders, directives, regulations and guidance.

1.1.3 The resources required to implement all information system security requirements shall be documented as a discrete line item in the programming and budgeting documentation.

1.1.4 Solicitation documentation for Agency information systems and services, to include information systems that will contain FIPS 199 Moderate or High security category NASA data, shall require documents that describe the functional properties of the security controls employed with sufficient detail to permit analysis and testing of the controls.

1.1.5 Documentation adequate to configure, install, and operate the information system shall be obtained, protected, and made available to authorized personnel.

1.1.6 Only approved and licensed software and associated documentation shall be acquired and used in accordance with contract agreements and copyright laws. NASA-STD-2804, Minimum Interoperability Software Suite, defines approved software for NASA desktops, including laptops, engineering workstations and similar platforms.

1.1.6.1 The use of public or internal Agency peer-to-peer file sharing software shall not be permitted unless specifically documented in the System Security Plan (SSP) and authorized by the Authorizing Official (AO).

1.1.6.2 The use of "Wiki" or equivalent technologies shall be approved only when the application is implemented and documented as part an information system that has full Certification and Accreditation (C&A) and meets NASA access management, authentication and authorization requirements in accordance with EA-STD-0001, Standard for Integrating Applications into the NASA Access Management, Authentication, and Authorization Infrastructure.

1.1.6.3 Approval/disapproval of Information Technology (IT) waivers to requirements in paragraph 1.1.6 shall be by the NASA Chief Information Officer (CIO) in accordance with the NASA Information Technology (IT) Waiver Process (Appendix C).

1.1.7 Binary or machine executable public domain software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware, shall not be used in NASA information systems, nor in systems processing NASA data, unless they are necessary for mission accomplishment and there are no alternative IT solutions available.

1.1.8 Software to be installed on NASA information systems shall be obtained from NASA approved sources. For example, desktop approved sources include the Outsourcing Desktop Initiative for NASA (ODIN) service provider and the Software Refresh Portal (SRP).

1.1.9 Contractor information systems that store and/or process NASA data shall:

a. Use Federal law, NIST guidelines, service level agreements, and NPR 2810.1, Security of Information Technology, in employing security controls.

b. Include security control compliance monitoring, documentation, and reporting in accordance with this security control, service level agreements and NPR 2810.1, Security of Information Technology.

1.1.10 NASA Federal Acquisition Regulation (FAR) supplement 1852-204-76, NASA Contract IT Security Clause, establishes the contractor requirements for contractor systems.

## **1.2 Procedures**

1.2.1. The ISO shall be responsible for assuring implementation of the above policy and procedures and document these procedures in the SSP.

1.2.2. The AO shall be responsible and accountable for the Agency risk for operation of the information system through the Authorization To Operate (ATO).

1.2.3. The Center Chief Information Officers (CIOs) shall be responsible for the security oversight, monitoring, assessment and reporting of cognizant contractor systems.

1.2.4. The Senior Agency Information Security Officer (SAISO) shall:

a. Annually review, and update as required, the Agency System and Services Acquisition Policy and Procedures as part of the annual review of the SA-1 control as an Agency common control.

b. Annually certify the SA-1 Agency common control to assure it satisfies the purpose, scope, and compliance requirements for system and services acquisition.

## APPENDIX A. Definitions

Term	Definition
Authorizing Official	A senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. [FIPS 200 adapted]
Certification	A confirmation in formal documentation that an accepted standard has been met.
Common Control	A security control that is inherited by an information system
Information System Owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (NIST; CNSS 4009, Adapted)
Peer-to Peer (P2P)	Computer network that uses diverse connectivity between participants in a network and the cumulative bandwidth of network participants rather than conventional centralized resources where a relatively low number of servers provide the core value to a service or application. P2P networks are typically used for connecting nodes via largely ad hoc connections
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544] Synonymous with Chief Information Security Officer (CISO)
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-18]
Wiki	A page or collection of Web pages designed to enable anyone who accesses it to contribute or modify content, using a simplified markup language



## **APPENDIX B. Acronyms**

AO	Authorizing Official
ATO	Authorization to Operate
CIO	Chief Information Officer
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
ISO	Information System Owner
IT	Information Technology
ITSM	Information Technology Security Manager
NAMS	NASA Account Management System
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
ODIN	Outsourcing Desktop Initiative for NASA
OMB	Office of Management and Budget
SA	System and Services Acquisition (A NIST family of security controls)
SAISO	Senior Agency Information Security Officer
SP	Special Publication
SRP	Software Refresh Portal
SSP	System Security Plan

## **APPENDIX C. NASA Information Technology (IT) Waiver Process**

### **Waivers to Information Technology (IT) Policies, Procedures, Standards, or Federal Requirements**

1. Waivers to IT policies, procedures, standards or requirements standards, shall be granted by the NASA CIO.
2. The NASA CIO may delegate authority and responsibility to Center CIOs for a specific type of IT waiver or for a specific program or issue.
  - 2.1. The NASA CIO delegation of waiver authority and responsibility shall be in writing for the specific delegated authority or be as specified in NASA policy directives, e.g. in an NPR.
3. The individual/office preparing the waiver request shall submit the waiver request to the cognizant Center CIO for Center CIO concurrence and action. Example: The Sounding Rocket Program at the Wallops Flight Facility would submit the waiver to the GFSC CIO for review and concurrence/non-concurrence.
4. The waiver request shall include:
  - 4.1 The NASA IT policy, procedure, standard, and/or Federal requirement to be waived.
  - 4.2 The reason and justification for the waiver is required including:
    - a. Risk Assessment;
    - b. Cost-Benefit Analysis;
    - c. Business Impact Assessment;
    - d. Identification of compensating controls/actions;
    - e. Proposed period of time for the waiver;
    - f. The proposed date by which the Center will be compliant with the NASA IT standard, security control, and/or Federal requirement; and
    - g. For an IT security control waiver or for any waiver that results in an unmitigated security weakness or deficiency, an Authorization Official (AO) approved Program of Action and Milestone (POA&M) shall be included with the waiver request.
5. The Center CIO shall evaluate the waiver and either concur or non-concur within 30 calendar days of receipt.

- a. Non-concurred waivers shall be returned to the requester.
- b. Non-concurred waivers may be escalated to the Center Director or designee.
- 6. The Center CIO will forward the waivers with concurrence to the NASA CIO.
- 7. The NASA CIO shall evaluate the waiver request and the Center concurrence and either approve or disapprove the request within 30 calendar days of receipt.
- 8. For waivers to requirements contained in NASA policy documents, this waiver process applies only to those policy documents for which the Office of the CIO is responsible. For waivers to requirements in NASA policy documents for which the NASA CIO is not responsible, the requester shall follow the waiver process called out in the NASA policy document itself.